REMARKS/ARGUMENTS

1. Claims

Claims 33-61 are pending in the application. Claims 33 and 59 have been amended as suggested by the Examiner. Favorable reconsideration of the application is respectfully requested in view of the following remarks.

2. Examiner's Response to Applicant's Arguments

In response to the last Office Action, Applicant argued that Wentker does not disclose the step of transmission of a single header followed by a plurality of payload messages each comprising a data block, where each data block is cryptographically verified upon receipt, and where the combination of payload blocks is verified. The effect of the novel feature is that software may efficiently and securely be loaded into the device even if the software is too large for the receiving device to be able to store it prior to installing it. By splitting up the payload in blocks and by cryptographically authenticating each individual payload block and a combination of all blocks upon receipt, the software is received efficiently in small blocks while authenticating each block as such as well as in relation to the entire payload. Hence, the data is loaded in small blocks, but only a single header is received without sacrificing the security with respect to the individual blocks and with respect to the entire payload, thereby ensuring that the received set of blocks belongs to and is authenticated against the issued package of blocks. In response, the Examiner, in the Final Office Action states:

> Applicant's arguments filed on 7/11/2008 have been fully considered but they are not persuasive. It is argued (page 11 of the remarks) that Wentker does not disclose "the step of transmission of a single header followed by a plurality of payload messages each comprising a data block, where each data block is cryptographically verified upon receipt, and where the combination of payload blocks is verified". Applicant's interpretation of the reference is noted. However, Wentker in figure 7c teaches transmitting the load command/header (step 364) first and once authenticated, plurality of payload messages/application (step 376) are transmitted. Furthermore, Wentker

teaches that each message comprises data block/DAP blocks (page 29 line 28-page 30 line 12 and figure 100) and each block is cryptographically verified and the combination thereof (page 10 lines 3-17, page 22 lines 8-24 and page 26 lines 3-24).

Applicant respectfully traverses the Examiner's interpretation of Wentker as applied to the present invention. Wentker discloses a load command that is being authenticated and then there follows one or more payload messages/applications where each such message has a data authentication pattern (DAP). This is technically different from the present invention wherein the first header has in its signature field the hash of a list of message digests (MDL in step 821) of the payload blocks P1 thru PN which is sent prior to sending the payload blocks. Thus the payload blocks do not to carry any authentication information at all in contrast to Wentker wherein the payload blocks each have a DAP.

Hence in the present invention, an MDL is created and protected by the header and the payload blocks are sent as they are. In contrast, in Wentker the payload block must be mapped onto messages that are each given a DAP. In the present invention, the chain of payloads are linked to the header in the sense that the blocks in the chain of payload blocks following after two different headers cannot be switched (when they differ). This is a result from the fact that the MDi values depend not only from the Pi but also from the previous payloads. In Wentker, the DAPs are created per payload as discussed at pages 21 and 22. Hence, the present invention differs technically from Wentker in how verification is realized and in what it achieves. In particular, the present invention the protection of the payloads is cryptographically linked to the header.

3. Claim Rejections – 35 U.S.C. § 102(b)

As noted above, Wentker fails to disclose all of the elements of the present invention. The solution according to claim 33 to the technical problem of providing the above effect is not disclosed nor hinted at in the cited prior art. In particular, the smart card of Wentker receives a load command and a subsequent load file where the load file may comprise a plurality of DAP blocks and one data block. However, a secure

loading of large applications while securing the authenticity and integrity of the individual blocks as well as the entire package is not addressed. Hence, the subject-matter of claim 33 involves an inventive step. The same arguments apply to the corresponding other independent claims. To anticipate, the prior art must teach all the claim elements and the claimed arrangement. Section 102 embodies the concept of novelty—if a device or process has been previously invented (and disclosed to the public), then it is not new, and therefore the claimed invention is "anticipated" by the prior invention. . . . Because the hallmark of anticipation is prior invention, the prior art reference—in order to anticipate under 35 U.S.C. § 102—must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements "arranged as in the claim." Consequently, the subject-matter of all independent claims is novel and non-obvious.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

Michael Cameron
Registration No. 50,298

Date: December 18, 2008

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-4145
mike.cameron@ericsson.com